

### REMARKS/ARGUMENTS

We disagree with the **overall conclusion of claims 1-19** being rejected under 25 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. We believe this invention is a new and useful business process.

Technology has evolved and become cheaper to use fingerprint image to identify individuals. Fingerprint scanners, the device drivers between the operating system and fingerprint scanner, the software application which takes the image (can be written in visual basic) and the image saved into a database is readily available (current process).

This has increased the usage of fingerprints images as a key which can open doors to facilities, and provide individuals access to web sites, such as online banks with financial information that can allow for the transfer of funds from one financial account to another account, changing userid and passwords on computer systems.

Additionally, the ability to “fake” a fingerprint such as a “gummy” fingerprint has gotten cheaper and easier to do. No technology exists which can detect “gummy” fingerprints. Detecting “gummy” fingerprints must be done manually. We propose to detect “gummy” fingerprints by adding to the above process (1) where the individual cleans the fingertips (can be done with a paper towel, a rough towel to dislodge “gummy” fingerprints, Note: cotton swap may or may not work depending if it’s a light swab or if its done roughly, and how good the quality of the material used in making the “gummy” fingerprint) and an individual to inspect the fingerprints (for enrollment – when the fingerprint image is first taken, and for authentication – when an individuals fingerprint image is taken and compared to the enrollment fingerprint image). Once an individual’s identity has been confirmed using their fingerprints, the individual is allowed to perform an action such as entering a building.

The San Antonio Express-News article, dated March 13, 2007 describes a real-world example where this invention can be useful. The article describes employees of Microsoft Corporation accessing or entering a company computer center, which contains computer servers selling company services, by the scanning of individual’s fingerprint. If the scanned fingerprint matches the fingerprint located in a database, possibly a Microsoft Access database), then the individual can enter the computer center building.

Using the current method described in the article of ensuring an individual, an employee of Microsoft Corporation with the authority to enter the facility, is who he or she is representing is unable to detect “fake” fingerprints. Our process can detect a fake fingerprint and prevent an unauthorized individual from entering the building.

Companies, such as Microsoft and Google, providing services or products over the internet have a need for this invention because they have computer centers with computer servers required for the selling of their services and products over the Internet. If an unauthorized person, a terrorist, is able to fake someone’s fingerprints and enter the computer center building, then the individual could destroy the computer servers. The

company's inability to sell their services or products could result in millions of dollars in losses. Financial markets would react to a publicly traded company loses by dropping their stock price. Investors would lose money as the company stock declined. If the company has a large number of stock outstanding, this could cause the financial markets to decline as investors sell other stock to cover their losses. Other investors seeing the decline in overall stock prices can react by selling their stock. The decline in the stock market could be severe enough to close the financial markets for two to three days. This would have an impact on a county's financial stability and in the general public's confidence in the economy. The risk of not implementing this new process can be devastating. This is why we believe **this invention is useful.**

This process is a departure from existing approaches in using fingerprints to identify an individual. In the past, fingerprint scanners have been used to identify individuals. However, they can be fooled in particular with the new technology process known as "gummy" fingerprints which can be easily created from fingerprints left on a cup. "Gummy" fingerprints at its low end form are equivalent to "gelatin" molds. The material used does not cause perspiration. To identify this type of fake fingerprints you need to check for changes in the color of a person's skin. Unfortunately, a good tan could be misidentified as a fake fingerprint. The other thoughts are to check for coldness of the finger. However, older people, due to bad circulation, have cold fingers which again could be misidentified as a fake fingerprint.

The approach to identifying fake fingerprints needs to change from one that is a passive technology, such as the reading of the fingerprint imprint to an active type of fingerprint scanner. The active type of fingerprint scanner would physically perform a function on the finger such trying to physically remove a gelatin mold on the fingertip. This is a new approach and no fingerprint scanner has been developed to perform this type of function. The risk involved with not being able to detect fingerprints in critical situations means that the function has to be done manually by an individual (referred to as an agent).

#### **Remarks on Cited References:**

Division of Forensic Science, Minimum Standards & Controls – The purpose of this document is a process for ensuring a clear, detailed fingerprint impression is taken. In section 16.3, it states it "requires the inspection of each area recorded to determine if the detail present is a clear & accurate depiction of the area that is being recorded." To ensure a clear impression is taken, on page 2 of 3 paragraph 2, discusses the use of alcohol to have clean, dry hands for depiction of all areas of the finger. There is no indication that this process is used to determine if an individual is using a "fake" fingerprint.

In the Kentucky State Police Inked Fingerprinting Techniques – It states "Fingers to be printed must be clean and dry." Alcohol swabs can be used to clean a finger to keep perspiration from being a problem. This is done to ensure a clear impression of the recorded area (for a better fingerprint image). Again, the purpose is not for identifying a "fake" fingerprint.

**Amendment to Background – Field of Invention**

[0003]

The method of the invention relates to increasing the ability to identify individuals using fingerprint readers by being able to identify individuals using “fake” fingerprints. The increase assurance of the individual’s identity allows them to perform actions such as entering a facility, ability to access web sites, changing or updating a password or Personal Identification Number (PIN). The specific field is security by being able to identify an individual through the use of fingerprints readers or scanners with a new business process.

~~The method of the invention relates to increasing the trust level associated with using fingerprint readers for the enrollment and authentication of an individual. The specific field includes information, security to include password or Personal Identification Number (PIN) updates, and biometrics (fingerprints).~~

**Amendment to Background – Description of Prior Art**

[0005]

Initially, fingerprints were taken manually by law enforcement organizations to identify individuals using their fingerprints. An individual would press their fingertips on an inkpad and then press their fingertips onto a piece of paper. As technology progressed, electronic fingerprint readers (for example, Precise Biometrics fingerprint reader, and Microsoft fingerprint reader) were developed to read an individual's fingerprint. The fingerprint reader's software (for example, the hardware device driver software which interfaces with a software application such as the Microsoft fingerprint reader DigitalPersona software application, or a custom software application) scans an individual's fingertips, and requests information on the individual whose fingertips have been scanned. The fingerprint reader's software then enters the information (fingertip scan with the individual's information) into a file, list, database (for example, the database can a Microsoft Access or Microsoft SQL database), or onto an integrated circuit card (smart card). This "enrollment" process creates the initial fingerprint template (a fingerprint image) in which other fingerprint scans will be compared against to determine an individual's identity and authorization for actions such as entering a facility.

[00012]

In summary, fingerprint readers can be fooled. Various methods have been developed which can authenticate an individual to access facilities or information through the use of "fake" fingerprints. A new approach to identifying "fake" fingerprints, based on today's technology, is needed. This will ensure the identity of the individual and their authorization for certain actions such as entering a facility, getting financial information over the Internet, changing computer passwords and userids.

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

By 

Irma Blancas  
936 Brady  
San Antonio, TX 78207  
(210) 433-~~7~~390

# Microsoft's center will power the Web

By L.A. LOREK

EXPRESS-NEWS BUSINESS WRITER

QUINCY, Wash. — While Microsoft Corp.'s just-built data center resembles one of the town's large produce processing plants, this server farm does not deal in fruit and vegetables.

Instead, the 470,000-square-foot beige structure houses computers that will deliver Web pages, e-mails, instant messages, photos, videos and software programs to the world's Internet surfers.

Few get to enter Microsoft's monolith.

Microsoft guards its design plans because the centers house extremely important data and corporate assets, said Mike Manos, the company's director of data centers.

Although the center doesn't go live until March 27, Microsoft allowed a sneak peak at its inner workings last month.

Microsoft doesn't even have a sign in front of its complex, but everyone in town knows where it's located. Microsoft is low-key compared to Yahoo, a few miles away, where a big sign marks its site.

The Microsoft building looks like a massive manufacturing plant, with a banklike security system. A perimeter fence and a security guard regulate who gets in and out.

Inside the main lobby, employees need badges with radio frequency identification smart chips to enter. Even with a badge, they still have to go through telephone-booth-sized revolving tubes in which they insert their hand into biometric scanner to gain entry.

Inside, a door to the right leads to a glass-enclosed main control room. Workers will oversee plant operations from there, but most of the 75 employees will sit at cubicles equipped with computers and monitors. A row of half a dozen closet-sized executive offices lines the back of the room with lime green and orange walls and multicolored carpeting. It's bright and cheerfully decorated in direct contrast to the rest of the plant.

Like the Internet, the center never closes, said Darrell

Amundson, the data center manager.

"We're prepared for everything," he said.

It's easy to get lost inside Microsoft's main building, which contains long halls with a tile floor and a maze of rooms centering around five 12,000-square-foot brain centers that contain tens of thousands of computer servers.

Each server room has two adjoining rooms lined with refrigerator-sized air-conditioning units to keep the temperature between 60 to 68 degrees Fahrenheit. Another room contains row after row of batteries to kick in for 18 seconds if a power failure should occur before the truck-sized backup generators fire up.

Microsoft locks the doors to the many of the rooms.

The center is quiet except for the soft murmur of air-conditioning systems and generators and the occasional construction worker completing a project. Thick walls make the buzz of the computers indiscernible from the outside hallway.

Aside from the computer systems, Microsoft also has a water treatment facility inside the plant and collects rainwater from its roof to use in its cooling system.

"With data centers it's better for us to be green," Manos said. "It ultimately means lower cost to us as an industry."

While the first building looks complete, a door at one side of the plant leads to a big construction area where workers are already putting up the shell of the next building. More than 30 construction trailers at the back of the property attest to the fact that work isn't over.

The San Antonio data center will look like a mirror copy of the Quincy site with a little bit of localization and improvements, Manos said. Yet Quincy has the ability to build six facilities and in San Antonio, Microsoft can only build two, he said.

"There's a sweet spot to doing this," Manos said. "You don't want to build them too big or too small."

SAN ANTONIO EXPRESS-NEWS

SUNDAY, MARCH 11, 2007



llorek@express-news.net

Attachment 1